

Large Cayley digraphs and bipartite Cayley digraphs of odd diameters

Marcel Abas^{a,*}, Tomáš Vetrík^b

^a*Institute of Applied Informatics, Automation and Mathematics,
Faculty of Materials Science and Technology in Trnava,
Slovak University of Technology in Bratislava, Trnava, Slovakia*

^b*Department of Mathematics and Applied Mathematics,
University of the Free State, Bloemfontein, South Africa*

Abstract

Let $C_{d,k}$ be the largest number of vertices in a Cayley digraph of degree d and diameter k , and let $BC_{d,k}$ be the largest order of a bipartite Cayley digraph for given d and k . For every degree $d \geq 2$ and for every odd k we construct Cayley digraphs of order $2k \left(\lfloor \frac{d}{2} \rfloor\right)^k$ and diameter at most k , where $k \geq 3$, and bipartite Cayley digraphs of order $2(k-1) \left(\lfloor \frac{d}{2} \rfloor\right)^{k-1}$ and diameter at most k , where $k \geq 5$. These constructions yield the bounds $C_{d,k} \geq 2k \left(\lfloor \frac{d}{2} \rfloor\right)^k$ for odd $k \geq 3$ and $d \geq \frac{3^k}{2^k} + 1$, and $BC_{d,k} \geq 2(k-1) \left(\lfloor \frac{d}{2} \rfloor\right)^{k-1}$ for odd $k \geq 5$ and $d \geq \frac{3^{k-1}}{k-1} + 1$. Our constructions give the best currently known bounds on the orders of large Cayley digraphs and bipartite Cayley digraphs of given degree and odd diameter $k \geq 5$. In our proofs we use new techniques based on properties of group automorphisms of direct products of abelian groups.

Keywords: Cayley digraph; Bipartite digraph; Degree; Diameter

1. Introduction

The study of large graphs of given degree and diameter has often been restricted to special classes of graphs. A particularly useful class is that of Cayley graphs, since their inherent symmetry enables to calculate their diameter by determining distances just from one vertex.

A directed Cayley graph (or simply Cayley digraph) $G = \text{Cay}(\Gamma, X)$ is specified by an *underlying* group Γ and by a unit-free *generating set* X for this group. Vertices of $\text{Cay}(\Gamma, X)$ are the elements of Γ , that is the vertex set $V(G)$ is equal to Γ , and there is a directed edge from the vertex u to the vertex v if and only if there is a generator $x \in X$ such that $ux = v$. Note that in a

*Corresponding author

Email addresses: abas@stuba.sk (Marcel Abas), vetrikt@ufs.ac.za (Tomáš Vetrík)

Cayley digraph all vertices have the same in-degree and out-degree, thus we will call this number the degree of the Cayley digraph. Since the mapping $\varphi_h : g \rightarrow hg, g \in V(G)$ is a digraph automorphism for every $h \in \Gamma$, Cayley digraphs are vertex-transitive.

We study Cayley digraphs of large order for given degree and diameter. Let $C_{d,k}$ be the largest number of vertices in a Cayley digraph of degree d and diameter k . Clearly, the number of vertices in a digraph of maximum degree d and diameter k can not exceed the *Moore bound* $M_{d,k} = 1 + d + d^2 + \dots + d^k$ and therefore $C_{d,k} \leq M_{d,k}$. Complete digraphs are the largest Cayley digraphs of diameter 1. They yield the result $C_{d,1} = M_{d,1} = d+1$. Ždímalová and Staneková [7] studied vertex-transitive digraphs of [2] and showed that $C_{d,2} = d^2 + d$ for $d = q - 1$, where $q \geq 3$ is a prime power, and $C_{d,3} \geq d^3 - d$, where $d \geq 3$ is a prime power. More general mixed Cayley graphs of diameter 2 were studied by Šiagiová [5]. In [6] it was proved that $C_{d,k} \geq k \left(\lfloor \frac{d}{2} \rfloor\right)^k$ for any $k \geq 3$ and $d \geq 4$. We improve this result for odd diameters. For odd $k \geq 3$ and for $d \geq 2$ we construct Cayley digraphs of order $2k \left(\lfloor \frac{d}{2} \rfloor\right)^k$, degree d and diameter at most k , and we show that $C_{d,k} \geq 2k \left(\lfloor \frac{d}{2} \rfloor\right)^k$ for each $d \geq \frac{3^k}{2^k} + 1$.

Now let us consider bipartite Cayley digraphs. Let $BC_{d,k}$ denote the largest possible number of vertices in a bipartite Cayley digraph of degree d and diameter k . Aider [1] showed that the number of vertices in a bipartite digraph is at most $2(1 + d^2 + \dots + d^{k-1})$ if k is odd, and $2d(1 + d^2 + \dots + d^{k-2})$ if k is even. The largest Cayley digraphs of diameter 2 are the complete bipartite digraphs, thus $BC_{d,2} = 2d$ for any $d \geq 2$. Constructions of bipartite Cayley digraphs presented in [6] yield the bounds $BC_{d,3} \geq 2d^2$ for $d \geq 2$, $BC_{d,k} \geq 2(k-1) \left(\lfloor \frac{d}{2} \rfloor\right)^{k-1}$ if $k \geq 4$ is even and $d \geq 4$ and $BC_{d,k} \geq (k-1) \left(\lfloor \frac{d}{2} \rfloor\right)^{k-1}$ if $k \geq 5$ is odd and $d \geq 4$. We present a construction of bipartite Cayley digraphs of order $2(k-1) \left(\lfloor \frac{d}{2} \rfloor\right)^{k-1}$, degree $d \geq 2$ and diameter at most k , where $k \geq 5$ is odd. For $d > \frac{3^{k-1}}{k-1} + 1$ we obtain the bound $BC_{d,k} \geq 2(k-1) \left(\lfloor \frac{d}{2} \rfloor\right)^{k-1}$.

2. Preliminaries

Let H be any additive abelian group of order n with unit element 0 and let $H^k = H \times H \times \dots \times H$ be the direct product of k copies of H . Elements of H^k will be written in the form $\vec{h} = (h_1, h_2, \dots, h_k)$, $h_i \in H$, $i \in \{1, 2, \dots, k\}$ and the group operation will be defined by $\vec{h} \cdot \vec{h}' = (h_1, h_2, \dots, h_k) \cdot (h'_1, h'_2, \dots, h'_k) = (h_1 + h'_1, h_2 + h'_2, \dots, h_k + h'_k)$.

Lemma 1. *Let $k = 2q + \epsilon$, where $q \geq 1$ is an integer, $\epsilon \in \{0, 1\}$, $k \neq 2$, and let $Sym(k)$ be the symmetric group on k symbols $1, 2, \dots, k$. Let $A_{q,\epsilon} = (1, 2, 3, \dots, k)$ be a k -cycle and let $B_{q,\epsilon}$ be products of the following disjoint transpositions:*

$B_{q,0} = (1, q)(2, q-1) \dots (\frac{q}{2}, \frac{q}{2} + 1)(q+1, k)(q+2, k-1) \dots (\frac{3q}{2}, \frac{3q}{2} + 1),$
 $B_{q,1} = (1, q)(2, q-1) \dots (\frac{q}{2}, \frac{q}{2} + 1)(q+1, k)(q+2, k-1) \dots (\frac{3q}{2}, \frac{3q}{2} + 2),$
for q even, and

$B_{q,0} = (1, q)(2, q-1) \dots (\frac{q+1}{2} - 1, \frac{q+1}{2} + 1)(q+1, k)(q+2, k-1) \dots (\frac{3q+1}{2} - 1, \frac{3q+1}{2} + 1),$
 $B_{q,1} = (1, q)(2, q-1) \dots (\frac{q+1}{2} - 1, \frac{q+1}{2} + 1)(q+1, k)(q+2, k-1) \dots (\frac{3q+1}{2}, \frac{3q+1}{2} + 1),$
 for q odd.
 Then the group $T_{q,\epsilon} = \langle A_{q,\epsilon}, B_{q,\epsilon} \rangle$ is isomorphic to the dihedral group D_k of order $2k$.

Proof. The dihedral group D_k of order $2k$ has the standard presentation in the form $D_k = \langle A, B | A^k = B^2 = 1, BAB = A^{-1} \rangle$. It is easy to verify that $A_{q,\epsilon}^k = I$, where k is the true order of $A_{q,\epsilon}$, $B_{q,\epsilon}^2 = I$ and that $B_{q,\epsilon} A_{q,\epsilon} B_{q,\epsilon} = (A_{q,\epsilon})^{-1}$. Since $A_{q,\epsilon}^i \neq A_{q,\epsilon}^j$ and $A_{q,\epsilon}^i B_{q,\epsilon} \neq A_{q,\epsilon}^j B_{q,\epsilon}$ for $i, j \in \{0, 1, \dots, k-1\}$, $i \neq j$, the group $T_{q,\epsilon}$ has order $2k$. Therefore the mapping $\psi : T_{q,\epsilon} \rightarrow D_k$ given by $A_{q,\epsilon} \rightarrow A$ and $B_{q,\epsilon} \rightarrow B$ is a group isomorphism. \square

Example 2. For the first four values of k we have:

$k = 3$ ($q = 1, \epsilon = 1$), $A_{1,1} = (123)$, $B_{1,1} = (23)$,
 $k = 4$ ($q = 2, \epsilon = 0$), $A_{2,0} = (1234)$, $B_{2,0} = (12)(34)$,
 $k = 5$ ($q = 2, \epsilon = 1$), $A_{2,1} = (12345)$, $B_{2,1} = (12)(35)$,
 $k = 6$ ($q = 3, \epsilon = 0$), $A_{3,0} = (123456)$, $B_{3,0} = (13)(46)$.

In what follows we will write D_k instead of $T_{q,\epsilon}$, where $D_k = T_{q,0}$ for k even and $D_k = T_{q,1}$ for odd k . Let $\Gamma_k = H^k \rtimes_{\varphi} D_k$ be a semidirect product of the group H^k and the group D_k represented as $T_{q,\epsilon}$. Note that to simplify the notation we will often omit the subscript k . Elements of Γ will be written in the form $\vec{h} \cdot C$, $\vec{h} \in H^k$, $C \in D_k$ and the product of two elements of Γ is given by:

$$\begin{aligned}
 \vec{h}C \cdot \vec{h}'C' &= (h_1, h_2, \dots, h_k)C \cdot (h'_1, h'_2, \dots, h'_k)C' \\
 &= (h_1 + h'_{C(1)}, h_2 + h'_{C(2)}, \dots, h_k + h'_{C(k)})CC',
 \end{aligned} \tag{1}$$

where CC' is the product of C and C' in D_k . In the homomorphism $\varphi : D_k \rightarrow \text{Aut}(H^k)$, elements of D_k induce permutations of coordinates of \vec{h} . If the order of H is n , then the group Γ has the order $|\Gamma| = 2kn^k$. For an element $g = \vec{h}C$ of Γ we say that \vec{h} is the *prefix* $P(g)$ of g and that C is the *suffix* $S(g)$ of g .

In what follows we will use the following notation for some special elements of Γ :

$$a(x) = (x, 0, \dots, 0)A, \quad x \in H, \tag{2}$$

where $A = A_{q,\epsilon}$ is the element of $T_{q,\epsilon}$ defined in Lemma 1, and

$$b(x) = (x, 0, \dots, 0, x, 0, \dots, 0)B, \quad x \in H, \tag{3}$$

where x occurs in the first and $(q+1)$ -st coordinate and $B = B_{q,\epsilon}$ is the element of $T_{q,\epsilon}$ defined in Lemma 1.

Let $\Gamma = H^k \rtimes_{\varphi} D_k$ be the underlying group and let $X = \{a(x), b(x) | x \in H\}$ be the generating set for the Cayley digraph $G = \text{Cay}(\Gamma, X)$. The graph G has degree $d = |X| = 2n$ and order $2kn^k = 2k \left(\frac{d}{2}\right)^k$, if d is even.

Let $w = C_1 C_2 \dots C_k$, $C_i \in \{A, B\}$, $i \in \{1, 2, \dots, k\}$, be a word in D_k . We say that the product $C = C_1 \cdot C_2 \cdot \dots \cdot C_k = V(w)$ is the *value* of the word w . The *fiber* over the word w is the set of all sequences $\gamma_1, \gamma_2, \dots, \gamma_k$ such that $\gamma_i = a(x_i)$ if $C_i = A$ and $\gamma_i = b(x_i)$ if $C_i = B$, $x_i \in H$. We denote the set of sequences by $\vec{\gamma}_w$ or simply by $\vec{\gamma}$. For given $\vec{x} \in H^k$, the *value* of $\vec{\gamma}_w(\vec{x})$ is the product $V(\vec{\gamma}(\vec{x})) = \gamma_1(x_1) \cdot \gamma_2(x_2) \cdot \dots \cdot \gamma_k(x_k)$.

Note that the previous definitions have a simple interpretation. If $G = \text{Cay}(\Gamma, X)$ is a Cayley digraph and w is a word in D_k , then the fiber $\vec{\gamma}_w$ over w is the set of all oriented walks of length k starting at 1_Γ and such that the vertices on the walks have suffices $C_1, C_1 \cdot C_2, C_1 \cdot C_2 \cdot C_3, \dots, C = V(w)$, respectively.

Since $V(\vec{\gamma}_w(\vec{x}))$ is an element of Γ , it has the form $V(\vec{\gamma}_w(\vec{x})) = \vec{z} \cdot C$, where $\vec{z} \in H^k$ and $C = V(w) \in D_k$. It is easy to see that for \vec{z} we have $\vec{z} = (z_1, z_2, \dots, z_k)$, where $z_i = m_{i,1}x_1 + m_{i,2}x_2 + \dots + m_{i,k}x_k$, such that $m_{i,j}$ is either 0 or 1 and that $m_{1,j} + m_{2,j} + \dots + m_{k,j}$ is equal to 1 if γ_i is $a(x_i)$ or 2 if γ_i is $b(x_i)$. Now, let

$$\begin{aligned} V(\vec{\gamma}_w(\vec{x})) &= (m_{1,1}x_1 + m_{1,2}x_2 + \dots + m_{1,k}x_k, \\ &\quad m_{2,1}x_1 + m_{2,2}x_2 + \dots + m_{2,k}x_k, \\ &\quad \vdots \\ &\quad m_{k,1}x_1 + m_{k,2}x_2 + \dots + m_{k,k}x_k) \cdot C. \end{aligned} \quad (4)$$

The *fiber matrix* over the word w is the square matrix $M = M(w)$ of degree k and of the form

$$M(w) = \begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,k} \\ m_{2,1} & m_{2,2} & \dots & m_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ m_{k,1} & m_{k,2} & \dots & m_{k,k} \end{pmatrix}. \quad (5)$$

Clearly, i -th row of M corresponds to the i -th coordinate of \vec{z} and j -th column of M corresponds to the j -th generator of $\vec{\gamma}_w(\vec{x})$.

Example 3. Let $q = 2$ and $\epsilon = 1$. Then $k = 2q + 1 = 5$, $a(x) = (x, 0, 0, 0, 0)A = (x, 0, 0, 0, 0)(12345)$ and $b(x) = (x, 0, x, 0, 0)B = (x, 0, x, 0, 0)(12)(35)$. If, for example, $w = ABBAB$, then $\vec{\gamma}_w(\vec{x}) = a(x_1)A, b(x_2)B, b(x_3)B, a(x_4)A, b(x_5)B$ and after a computation we have $V(\vec{\gamma}_w(\vec{x})) = a(x_1)A \cdot b(x_2)B \cdot b(x_3)B \cdot a(x_4)A \cdot b(x_5)B = (x_1 + x_3, x_2 + x_4, x_3 + x_5, x_2, x_5) \cdot A^2B$. The fiber matrix over the word

$$w \text{ is } M(w) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

One sees that for given word w and for the fiber matrix $M = M(w)$ over w we have $P(V(\vec{\gamma}_w(\vec{x}))) = (M\vec{x}^T)^T = \vec{x}M^T$ (note that $P(g)$ is the prefix of g).

Definition 4. We say that the fiber $\vec{\gamma}_w$ over the word w covers the element $C = V(w)$ of D_k if for every $\vec{y} = (y_1, y_2, \dots, y_k) \in H^k$ there is a vector $\vec{x} = (x_1, x_2, \dots, x_k) \in H^k$ such that $M\vec{x}^T = \vec{y}^T$.

The definition says that $\vec{\gamma}_w$ covers $C = V(w)$ if for every vertex g of $G = \text{Cay}(\Gamma, X)$ with suffix $S(g) = C$ there is an oriented walk of length k from 1_Γ to the vertex g such that the vertices on the walk have suffices $C_1, C_1 \cdot C_2, \dots, C = V(w)$.

Lemma 5. Let $\vec{\gamma}_w$ cover $C = V(w)$ and let $\vec{y}_0 \in H^k$. Then there exists exactly one $\vec{x}_0 \in H^k$ such that $M\vec{x}_0^T = \vec{y}_0^T$.

Proof. Since $\vec{\gamma}_w$ covers C , for every $\vec{y}_0 \in H^k$ there exists a vector $\vec{x}_0 \in H^k$ such that $M\vec{x}_0^T = \vec{y}_0^T$. Now we show that this \vec{x}_0 is unique.

In the Cayley digraph $G = \text{Cay}(\Gamma, X)$ there are exactly n^k vertices of the form $\vec{x}C$. The lemma in fact says that for every vertex $g \in G$ of the form $g = \vec{x}C$ there is exactly one oriented walk from 1_Γ to g such that the suffices of the vertices g_1, g_2, \dots, g_k , where $g_k = g$, on the walk are the elements $C_1, C_1 \cdot C_2, \dots, C = V(w)$ of D_k . Since the group H has order n , there is at most n^k terminal vertices of $\vec{\gamma}_w$. On the other hand, every vertex with suffix C (its number is also n^k) is reachable from 1_Γ by a walk $\vec{\gamma}_w(\vec{x}_0)$ (since $\vec{\gamma}$ covers C). \square

Corollary 6. Let $\vec{\gamma}_w$ cover $C = V(w)$ and let M be the fiber matrix over w . Then the mapping $\mu : H^k \rightarrow H^k$ given by $\mu(\vec{x}) = \vec{x}M^T$ is a group automorphism.

Proof. By Definition 4, for every $\vec{y} \in H^k$ there is a vector $\vec{x} \in H^k$ such that $\mu(\vec{x}) = \vec{y}$ and by Lemma 5 the mapping μ is a bijection. It is easy to see that for $\vec{x} = \vec{x}_1 + \vec{x}_2$ we have $\mu(\vec{x}_1 + \vec{x}_2) = \mu(\vec{x}) = \vec{x}M^T = (\vec{x}_1 + \vec{x}_2)M^T = \vec{x}_1M^T + \vec{x}_2M^T = \mu(\vec{x}_1) + \mu(\vec{x}_2)$. Therefore μ is a bijective group endomorphism of the group H^k and therefore a group automorphism. \square

Definition 7. We say that a column j (row i) of a matrix M is of *type I* if it contains exactly one unit and it is of *type II* if it contains two (two or more) 1's.

Lemma 8. Let M be a zero-one matrix of order $k \geq 1$ with $\det(M) = \pm 1$ such that in any column of M there are at most two 1's. Then there is at least one row of type I in M .

Proof. Let $l \in \{0, \dots, k\}$ be the number of columns of type II in M . The assertion is true for $k = 1$ and for every $k > 1$, $l < k$. For $k = l = 2$ the determinant of M is equal to 0. Now let $l = k \geq 3$. If there is no row of type I, then in every row of the matrix there are exactly two '1'-s. Therefore we have a zero-one matrix of order $k \geq 3$ with equal row and column sum 2. It is easy to verify that the determinant of such a matrix is an even number – a contradiction. \square

Lemma 9. Let w be a word in D_k and let the fiber matrix $M = M(w)$ be a matrix with $\det(M) = \pm 1$. Then $\vec{\gamma}_w$ covers $C = V(w)$.

Proof. It is sufficient to show that for every pair of different elements $\vec{x}_0 \neq \vec{x}_1$ of H^k we have $M\vec{x}_0^T \neq M\vec{x}_1^T$. We prove the lemma by a contradiction. Let $\vec{x}_0 \neq \vec{x}_1$ and \vec{y}_0 in H^k be such that $M\vec{x}_0^T = M\vec{x}_1^T = \vec{y}_0^T$. That is, $M\vec{x}^T = \vec{0}^T$ for some non-zero vector \vec{x} of H^k . Since M is a zero-one matrix with determinant ± 1 and such that there are at most two 1's in any column of M , there is (by Lemma 8) at least one row, say i , of type I in M . Let the 1 of this row be in a column j . The 1 is the only 1 in the row, thus from the definition of fiber matrix it follows that to get $y_i = 0$ we have to set $x_j = 0$. Now we can omit the row i and the column j to get a new matrix M' (corresponding to a new mapping $M' : H^{k-1} \rightarrow H^{k-1}$). Since M' is again a zero-one matrix with determinant ± 1 and with at most two 1's in any column, there is at least one row of type I in M' and we can continue with the process. In this way, after $(k-1)$ steps, we get 1×1 matrix \tilde{M} with entry $\tilde{m}_{1,1} = 1$. The entry corresponds to a row i' and column j' of M . To obtain $y_{i'} = 0$ we have to set $x_{j'} = 0$. Therefore \vec{x} is the zero vector of H^k – a contradiction. \square

Note 10. We have already seen that if $\vec{\gamma}_w$ covers $V(w)$, then the mapping $\mu(\vec{x}) = \vec{x}M^T$ is a group automorphism. Lemma 9 in fact says, that if M has $\det(M) = \pm 1$, then the mapping $\mu(\vec{x}) = \vec{x}M^T$ is a group automorphism as well.

3. Results

In this section we study products of $k = 2q + \epsilon$, $\epsilon \in \{0, 1\}$, generators (elements of X) in terms of matrices $M(w)$ over the corresponding word w . More precisely, for a given set S of elements of D_k , for each $C \in S$ we find a word w in D_k such that $V(w) = C$ and the fiber matrix M over w has determinant equal to ± 1 .

To simplify the notation, in the lemmas that follow we will write $a(i)$ for the generator which yields the column of M with the i -th entry equal to 1, $1 \leq i \leq k$. Similarly, we will write $b(j, j')$ for the generator with the j -th and j' -th entry equal to 1, $1 \leq j < j' \leq k$. For example, let us have $q = 2$, $\epsilon = 1$ and $w = ABBAB$ as in Example 3. Then $a(x_1)b(x_2)b(x_3)a(x_4)b(x_5)$ corresponds to $(x_1 + x_3, x_2 + x_4, x_3 + x_5, x_2, x_5)A^2B$ and we simply write $\vec{\gamma}_w \rightarrow a(1)b(2, 4)b(1, 3)a(2)b(3, 5)$ instead. Note that i, j and j' in $a(i)$ and $b(j, j')$ are determined by the product of preceding generators.

3.1. Cayley digraphs

In the next lemma, for any element $A^p B^l$ of the group D_k , k odd, $p \in \{1, 2, \dots, k\}$ and $l \in \{0, 1\}$, we present a sequence of k generators (a word in D_k) whose product is the element with suffix $A^p B^l$ and the corresponding matrix M has determinant ± 1 .

Lemma 11. *Let $q \geq 1$ be an integer and let $k = 2q + 1$. Then for every C in D_k there is a word w in D_k such that $V(w) = C$ and the fiber matrix $M(w)$ over the word w is a matrix with $\det(M) = \pm 1$.*

Proof. All the elements of D_k are of the form $A^p B^l$, $p \in \{1, 2, \dots, k\}$, $l \in \{0, 1\}$ and we distinguish eight cases i), ii), ..., viii), depending on the values of p and l . In the first four cases $V(w) = A^p$ and in the last four cases $V(w) = A^p B$.

i) $l = 0$, p even, $q + 1 \leq p \leq 2q$, $V(w) = A^p$, where

$$w = B \underbrace{AABB}_{[(q-p/2)-\text{times}]} \underbrace{A}_{[(p-q)-\text{times}]} B \underbrace{A}_{[(p-q-1)-\text{times}]}.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow b(1, q+1) \\ &\quad [a(q)a(q-1)b(q-2, 2q-1)b(q-1, 2q) \\ &\quad a(q-2)a(q-3)b(q-4, 2q-3)b(q-3, 2q-2) \\ &\quad \vdots \\ &\quad a(p-q+2)a(p-q+1)b(p-q, p+1)b(p-q+1, p+2)] \\ &\quad a(p-q)a(p-q-1) \dots a(1) \\ &\quad b(q+1, 2q+1) \\ &\quad a(q+2)a(q+3) \dots a(p) \end{aligned} \tag{6}$$

Consider a column of M containing only one entry 1. If we remove the row and column in which this entry appears, we obtain a new square matrix of degree $2q = k - 1$ whose determinant is equal to $\pm \det(M)$. Since there are $(p - 1)$ generators $a(i)$ in the expression (6), we have $(p - 1)$ columns with the only non-zero entry. All these $(p - 1)$ non-zero entries are in different rows. We delete rows and columns which correspond to these non-zero entries to get a new square matrix, say M' , of degree $2q - p + 2$. We have $\det(M') = \pm \det(M)$. Note that the new matrix M' contains the rows $q + 1, p + 1, p + 2, \dots, 2q + 1$ of the matrix M and the only generator which yields a column of M' with two entries equal to 1 is $b(q + 1, 2q + 1)$. The generator $b(q + 1, 2q + 1)$ corresponds to the last $(2q - p + 2)$ -th column of M' and the $(q + 1)$ -th row of M corresponds to the first row of M' . Except for the first row and the last column of M' , every row and every column of M' contains exactly one non-zero entry, which implies that $\det(M') = \pm 1$.

To give an example of this situation, let $q = 5$ and $p = 6$. Then $k = 11$, $w = BAABBAABBAB$, $V(w) = A^6$,
 $\vec{\gamma}_w \rightarrow b(1, 6)a(5)a(4)b(3, 9)b(4, 10)a(3)a(2)b(1, 7)b(2, 8)a(1)b(6, 11),$

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } M' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

ii) $l = 0$, p even, $2 \leq p \leq q$, $V(w) = A^p$, where

$$w = B \underbrace{A}_{[(q-p+2)\text{-times}]} \underbrace{ABBA}_{[(p/2-1)\text{-times}]} \underbrace{A}_{[(q-p+1)\text{-times}]} B.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow b(1, q+1) \\ &\quad a(q)a(q-1) \dots a(p-1) \\ &\quad [a(p-2)b(p-3, p+q-2)b(p-2, p+q-1)a(p-3) \\ &\quad a(p-4)b(p-5, p+q-4)b(p-4, p+q-3)a(p-5) \\ &\quad \vdots \\ &\quad a(2)b(1, q+2)b(2, q+3)a(1)] \\ &\quad a(2q+1)a(2q) \dots a(p+q+1) \\ &\quad b(p, p+q) \end{aligned} \tag{7}$$

Let us note that non-zero entries in the matrix M corresponding to the generators $a(i)$ appear in the rows: $1, 2, \dots, q$ and $p+q+1, p+q+2, \dots, 2q+1$. We remove these rows from M together with columns corresponding to generators $a(i)$ to create a square matrix M' of order p , such that $\det(M') = \pm \det(M)$.

For every generator $b(j, j')$ appearing in the expression (7), j -th row does not appear in M' and j' -th row appears in M' . It follows that each column of M' contains exactly one non-zero entry. Since any two j' -s are different, each row of M' contains exactly one non-zero entry as well. Hence $\det(M') = \pm 1$.

iii) $l = 0$, p odd, $q+1 \leq p \leq 2q+1$, $V(w) = A^p$, where

$$w = \underbrace{A}_{[(p-q-1)\text{-times}]} \underbrace{AABB}_{[(q+1-(p+1)/2)\text{-times}]} \underbrace{A}_{[(p-q)\text{-times}]} B.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow a(1)a(2) \dots a(p-q-1) \\ &\quad [a(p-q)a(p-q+1)b(p-q+2, p+2)b(p-q+1, p+1) \\ &\quad a(p-q+2)a(p-q+3)b(p-q+4, p+4)b(p-q+3, p+3) \\ &\quad \vdots \\ &\quad a(q-1)a(q)b(q+1, 2q+1)b(q, 2q)] \\ &\quad a(q+1)a(q+2) \dots a(p) \end{aligned} \tag{8}$$

We study the matrix M corresponding to this product of generators. We focus on those entries 1 in the matrix M , which lie in columns corresponding to the generators $a(i)$. We again create a new matrix M' by removal of columns and rows of M , in which these entries 1 appear to obtain a new square matrix of degree $2q - p + 1$. Note that we removed first p rows of M . It follows that $\det(M') = \pm \det(M)$. The matrix M' has exactly one non-zero entry in each column and in each row, and so $\det(M') = \pm 1$.

iv) $l = 0$, p odd, $1 \leq p \leq q$, $V(w) = A^p$, where

$$w = B \underbrace{A}_{[(q-p)\text{-times}]} B \underbrace{A}_{[(q-p)\text{-times}]} \underbrace{AABB}_{[((p-1)/2)\text{-times}]} A.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow b(1, q+1) \\ &\quad a(q)a(q-1) \dots a(p+1) \\ &\quad b(p, p+q+1) \\ &\quad a(p+q+2)a(p+q+3) \dots a(2q+1) \\ &\quad [a(1)a(2)b(3, q+3)b(2, q+2) \\ &\quad a(3)a(4)b(5, q+5)b(4, q+4) \\ &\quad \vdots \\ &\quad a(p-2)a(p-1)b(p, p+q)b(p-1, p+q-1)] \\ &\quad a(p) \end{aligned} \tag{9}$$

v) $l = 1$, p even, $q+1 \leq p \leq 2q$, $V(w) = A^p B$, where

$$w = \underbrace{A}_{[(p-q)\text{-times}]} \underbrace{AABB}_{[(q-p/2)\text{-times}]} \underbrace{A}_{[(p-q)\text{-times}]} B.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow a(1)a(2) \dots a(p-q) \\ &\quad [a(p-q+1)a(p-q+2)b(p-q+3, p+3)b(p-q+2, p+2) \\ &\quad a(p-q+3)a(p-q+4)b(p-q+5, p+5)b(p-q+4, p+4) \\ &\quad \vdots \\ &\quad a(q-1)a(q)b(q+1, 2q+1)b(q, 2q)] \\ &\quad a(q+1)a(q+2) \dots a(p) \\ &\quad b(p-q, q+1) \end{aligned} \tag{10}$$

$$\text{vi)} \ l = 1, p \text{ even}, 2 \leq p \leq q, V(w) = A^p B, \text{ where}$$

$$w = A \underbrace{AABB}_{[(p/2-1)\text{-times}]} \underbrace{A}_{[(q-p+2)\text{-times}]} B \underbrace{A}_{[(q-p+1)\text{-times}]}.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow a(1) \\ &\quad [a(2)a(3)b(4, q+4)b(3, q+3) \\ &\quad a(4)a(5)b(6, q+6)b(5, q+5) \\ &\quad \vdots \\ &\quad a(p-2)a(p-1)b(p, p+q)b(p-1, p+q-1)] \\ &\quad a(p)a(p+1) \dots a(q+1) \\ &\quad b(1, q+2) \\ &\quad a(2q+1)a(2q) \dots a(p+q+1) \end{aligned} \quad (11)$$

$$\text{vii)} \ l = 1, p \text{ odd}, q+2 \leq p \leq 2q+1, V(w) = A^p B, \text{ where}$$

$$w = \underbrace{A}_{[(p-q-1)\text{-times}]} B \underbrace{A}_{[(p-q-1)\text{-times}]} \underbrace{ABBA}_{[(q-(p-1)/2)\text{-times}]}.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow a(1)a(2) \dots a(p-q-1) \\ &\quad b(p-q, p) \\ &\quad a(p-1)a(p-2) \dots a(q+1) \\ &\quad [a(q)b(q-1, 2q)b(q, 2q+1)a(q-1) \\ &\quad a(q-2)b(q-3, 2q-2)b(q-2, 2q-1)a(q-3) \\ &\quad \vdots \\ &\quad a(p-q+1)b(p-q, p+1)b(p-q+1, p+2)a(p-q)] \end{aligned} \quad (12)$$

$$\text{viii)} \ l = 1, p \text{ odd}, 1 \leq p \leq q+1, V(w) = A^p B, \text{ where}$$

$$w = B \underbrace{A}_{[(q-p+1)\text{-times}]} \underbrace{ABBA}_{[(p-1)/2\text{-times}]} \underbrace{A}_{[(q-p+1)\text{-times}]}.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow b(1, q+1) \\ &\quad a(q)a(q-1) \dots a(p) \\ &\quad [a(p-1)b(p-2, p+q-1)b(p-1, p+q)a(p-2) \\ &\quad a(p-3)b(p-4, p+q-3)b(p-3, p+q-2)a(p-4) \\ &\quad \vdots \\ &\quad a(2)b(1, q+2)b(2, q+3)a(1)] \\ &\quad a(2q+1)a(2q) \dots a(p+q+1) \end{aligned} \quad (13)$$

In the cases iv) - viii) we can obtain the matrices M and M' analogously as in the cases i), ii) and iii). Note that in each case except for the first one, the matrix M' has exactly one non-zero entry in every row and in every column, which implies that $\det(M) = \pm 1$. \square

Theorem 12. *For every odd $k \geq 3$ and for every even $d \geq 2$ there exists a Cayley digraph of order $2k(\frac{d}{2})^k$, degree d and diameter at most k .*

Proof. Let H be an abelian group of order $n \geq 1$ and let $\Gamma_k = H^k \rtimes_{\varphi} D_k$. Let $G = \text{Cay}(\Gamma_k, X)$ be the Cayley digraph for the underlying group Γ_k and for the generating set $X = \{a(x), b(x) | x \in H\}$ introduced in Preliminaries. Since $|X| = 2n$, the Cayley digraph G has degree $d = 2n$ and the order of G is $2kn^k = 2k(\frac{d}{2})^k$. To show that G has diameter at most k it is sufficient to show that every element of Γ_k is a product of at most k elements of X . Let $C \in D_k$. By Lemma 11 for every $C \in D_k$ there is a word w in D_k such that the fiber matrix over w has determinant equal to ± 1 . By Lemma 9 the fiber over w covers the element $C = V(w)$ of D_k , that is every element of Γ_k with suffix C is a product of k elements of X . Therefore the diameter of G is at most k . \square

Corollary 13. *For any odd $k \geq 3$ and for any $d \geq 2$ there exists a Cayley digraph of order $2k \left(\lfloor \frac{d}{2} \rfloor\right)^k$, degree d and diameter at most k .*

Proof. Adding one additional generator to the generating set X presented in the proof of Theorem 12, cannot increase the diameter. Therefore we obtain a Cayley digraph of degree $d = 2n + 1$, order $2kn^k = 2k(\frac{d-1}{2})^k$ and diameter at most k . \square

Theorem 14 (Main theorem for Cayley digraphs). *Let $k \geq 3$ be odd and let $d \geq \frac{3^k}{2^k} + 1$. Then $C_{d,k} \geq 2k \left(\lfloor \frac{d}{2} \rfloor\right)^k$.*

Proof. We show that for $d \geq \frac{3^k}{2^k} + 1$, the Cayley digraphs described in the proofs of Theorem 12 and Corollary 13 have diameter k . The maximum order of a digraph of degree d and diameter $k \leq k-1$ is $M_{d,k-1} = 1 + d + d^2 + \dots + d^{k-1} = \frac{d^k - 1}{d - 1}$, therefore it is sufficient to show that for $d \geq \frac{3^k}{2^k} + 1$ the orders of the Cayley digraphs are greater than the Moore bound for digraphs of diameter $k-1$. That is, if $2k \left(\lfloor \frac{d}{2} \rfloor\right)^k > \frac{d^k - 1}{d - 1}$, then the Cayley digraphs have diameter exactly k . We distinguish two cases.

i) $d \geq 2$ is even:

From the inequality $2k \left(\frac{d}{2}\right)^k > \frac{d^k - 1}{d - 1}$ we get $d > \frac{2^k}{2^k} - \frac{1}{2^k} \left(\frac{2}{d}\right)^k + 1$. Since $-\frac{1}{2^k} \left(\frac{2}{d}\right)^k < 0$, we obtain that if $d \geq \frac{2^k}{2^k} + 1$, then the Cayley digraph has diameter exactly k .

ii) $d \geq 3$ is odd:

From $2k \left(\frac{d-1}{2}\right)^k > \frac{d^k - 1}{d - 1}$ we have $d > \left(\frac{d-1}{2}\right)^k \frac{2^k}{2^k} - \frac{1}{2^k} \left(\frac{2}{d-1}\right)^k + 1$. Clearly $-\frac{1}{2^k} \left(\frac{2}{d-1}\right)^k < 0$ and $\frac{d}{d-1} \leq \frac{3}{2}$, thus if $d \geq \frac{3^k}{2^k} + 1$, the diameter of the Cayley digraph is exactly k . \square

3.2. Bipartite Cayley digraphs

In the next lemma, for any element $A^p B$ (A^{p+1}) of the group D_k , k even, $p \in \{1, 3, 5, \dots, k-1\}$, we present a sequence of k generators (a word in D_k)

whose product is the element with suffix $A^p B$ (A^{p+1}) and with the corresponding matrix M with determinant ± 1 .

Lemma 15. *Let $q \geq 2$ be an integer and let $k = 2q$. Then for every $C \in \{A^p B, A^{p+1} | 1 \leq p \leq k-1, p \text{ odd}\}$, $C \in D_k$, there is a word w in D_k such that $V(w) = C$ and the fiber matrix $M(w)$ over the word w is a matrix with $\det(M) = \pm 1$.*

Proof. We distinguish four cases: i), ii) for $C = A^{p+1}$ and iii), iv) for $C = A^p B$. In the first two cases we will use the notation $p' = p+1$, p' even.

i) $q \leq p' \leq 2q$, $V(w) = A^{p'}$, where

$$w = \underbrace{A}_{[(p'-q)\text{-times}]} \underbrace{ABBA}_{[(2q-p'/2)\text{-times}]} \underbrace{A}_{[(p'-q)\text{-times}]}.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow a(1)a(2)\dots a(p'-q) \\ &\quad [a(p'-q+1)b(p'-q+2, p+2)b(p'-q+1, p+1)a(p'-q+2) \\ &\quad a(p'-q+3)b(p'-q+4, p+4)b(p'-q+3, p+3)a(p'-q+4) \\ &\quad \vdots \\ &\quad a(q-1)b(q, 2q)b(q-1, 2q-1)a(q)] \\ &\quad a(q+1)a(q+2)\dots a(p') \end{aligned} \tag{14}$$

It can be checked that, in (14), non-zero entries of generators $a(i)$ appear in the rows $1, 2, \dots, p'$. We remove from M rows and columns in which these non-zero entries appear to obtain a new square matrix M' of degree $2q - p'$, where $\det(M') = \pm \det(M)$. Columns of M' correspond to generators $b(j, j')$. Note that the j -th row of M does not appear in M' , and the j' -th row of M appears in M' . Hence M' has exactly one non-zero element in each row and in each column, which implies that $\det(M') = \pm 1$.

For the remaining cases we list the corresponding instances and then append a note of how they can be handled.

$$\text{ii) } 2 \leq p' \leq q-1, V(w) = A^{p'}, \text{ where} \\ w = B \underbrace{A}_{[(q-p'+2)-\text{times}]} \underbrace{BBAA}_{[(p'/2-1)-\text{times}]} \underbrace{A}_{[(q-p')-\text{times}]} B.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow b(1, q+1) \\ &a(q)a(q-1) \dots a(p'-1) \\ &[b(p'-2, p'+q-2)b(p'-1, p'+q-1)a(p'-2)a(p'-3) \\ &b(p'-4, p'+q-4)b(p'-3, p'+q-3)a(p'-4)a(p'-5) \\ &\vdots \\ &b(2, q+2)b(3, q+3)a(2)a(1)] \\ &a(2q)a(2q-1) \dots a(p'+q+1) \\ &b(p', p'+q) \end{aligned} \tag{15}$$

$$\text{iii) } 1 \leq p \leq q, V(w) = A^p B, \text{ where} \\ w = B \underbrace{A}_{[(q-p+1)-\text{times}]} \underbrace{BBAA}_{[(p-1)/2-\text{times}]} \underbrace{A}_{[(q-p)-\text{times}]} .$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow b(1, q+1) \\ &a(q)a(q-1) \dots a(p) \\ &[b(p-1, p+q-1)b(p, p+q)a(p-1)a(p-2) \\ &b(p-3, p+q-3)b(p-2, p+q-2)a(p-3)a(p-4) \\ &\vdots \\ &b(2, q+2)b(3, q+3)a(2)a(1)] \\ &a(2q)a(2q-1) \dots a(p+q+1) \end{aligned} \tag{16}$$

$$\text{iv) } q+1 \leq p \leq 2q-1, V(w) = A^p B, \text{ where} \\ w = \underbrace{A}_{[(p-q)-\text{times}]} \underbrace{AABB}_{[(q-(p+1)/2)-\text{times}]} \underbrace{A}_{[(p-q+1)-\text{times}]} B.$$

$$\begin{aligned} \vec{\gamma}_w &\rightarrow a(1)a(2) \dots a(p-q) \\ &[a(p-q+1)a(p-q+2)b(p-q+3, p+3)b(p-q+2, p+2) \\ &a(p-q+3)a(p-q+4)b(p-q+5, p+5)b(p-q+4, p+4) \\ &\vdots \\ &a(q-2)a(q-1)b(q, 2q)b(q-1, 2q-1)] \\ &a(q)a(q+1) \dots a(p) \\ &b(p-q+1, p+1) \end{aligned} \tag{17}$$

In a way similar to what was presented in the case i) one can show that determinants of matrices corresponding to the products (15), (16) and (17) are 1 or -1. \square

Theorem 16. *For every odd $k \geq 5$ and for every even $d \geq 2$ there exists a bipartite Cayley digraph of order $2(k-1) \left(\frac{d}{2}\right)^{k-1}$, degree d and diameter at most k .*

Proof. Let $k' = k - 1$, let $n \geq 1$ be an integer, let H be an abelian group of order n and let $\Gamma_{k'} = H^{k'} \rtimes_{\varphi} D_{k'}$. Let $G = \text{Cay}(\Gamma_{k'}, X)$ be the Cayley digraph for the underlying group $\Gamma_{k'}$ and for the generating set $X = \{a(x), b(x) | x \in H\}$ introduced in Preliminaries. Since $|X| = 2n$, the Cayley digraph has degree $d = 2n$ and the order of the Cayley digraph is $2k'n^{k'} = 2k' \left(\frac{d}{2}\right)^{k'}$. To show that G has diameter at most k it is sufficient to show that every element of $\Gamma_{k'}$ is a product of at most k elements of X . Let $S = \{A^p B, A^{p+1} | 1 \leq p \leq k', p \text{ odd}\}$ and let $C \in S$. By Lemma 15 for every $C \in S$ there is a word w in $D_{k'}$ such that the fiber matrix over w has determinant equal to ± 1 . By Lemma 9 the fiber over w covers the element $C = V(w)$ of S , that is every element of $\Gamma_{k'}$ with suffix $C \in S$ is a product of k' elements of X . Since generators from X have suffices either A or B , no vertex with suffix A^l is adjacent to the vertex with suffix $A^m B$ if one of l, m is even and the other one is odd. Also no vertex with suffix $A^l B^i$ is adjacent to the vertex with suffix $A^m B^i$ for $i = 0$ or 1 , if both, l, m are even, or if both l, m are odd. Therefore the Cayley digraph G is bipartite. Note that in a bipartite Cayley digraph, if one can obtain any vertex in one part as a product of k' generators, then all vertices in the other part can be obtained as products of (at most) $k' + 1 = k$ generators. Therefore the diameter of G is at most k . \square

Corollary 17. *For every odd $k \geq 5$ and for every $d \geq 2$ there exists a bipartite Cayley digraph of order $2(k-1) \left(\left\lfloor \frac{d}{2} \right\rfloor\right)^{k-1}$, degree d and diameter at most k .*

Proof. We add one additional generator with suffix A to the generating set X given in the proof of Theorem 16 to obtain a Cayley digraph which is still bipartite and has the diameter at most k . We thus obtain a bipartite Cayley digraph of degree $d = 2n + 1$, order $2(k-1)n^{k-1} = 2(k-1) \left(\left\lfloor \frac{d}{2} \right\rfloor\right)^{k-1}$ and diameter at most k . \square

Theorem 18 (Main theorem for bipartite Cayley digraphs). *Let $k \geq 5$ be odd and let $d \geq \frac{3^{k-1}}{k-1} + 1$. Then $BC_{d,k} \geq 2(k-1) \left(\left\lfloor \frac{d}{2} \right\rfloor\right)^{k-1}$.*

Proof. Let $d \geq \frac{3^{k-1}}{k-1} + 1$. Let us prove that the bipartite Cayley digraphs described in the proofs of Theorem 16 and Corollary 17 are of diameter k . Since k is odd, the order of a bipartite digraph of diameter $\tilde{k} \leq k-1$ cannot exceed the bound $MB_{d,k-1} = 2d(1 + d^2 + d^4 + \dots + d^{k-2}) = 2d \frac{d^{k-1}-1}{d^2-1}$. Thus it suffices to show that if $d \geq \frac{3^{k-1}}{k-1} + 1$, then the orders of our bipartite Cayley digraphs are greater than the Moore bound for bipartite digraphs of diameter $k-1$. That is, if $2(k-1) \left(\left\lfloor \frac{d}{2} \right\rfloor\right)^{k-1} > 2d \frac{d^{k-1}-1}{d^2-1}$, then the Cayley digraphs are of diameter exactly k . Let us consider two cases.

i) $d \geq 2$ is even:

From $2(k-1) \left(\frac{d}{2}\right)^{k-1} > 2d \frac{d^{k-1}-1}{d^2-1}$ we have $d > \frac{2^{k-1}}{k-1} - \frac{1}{k-1} \left(\frac{2}{d}\right)^{k-1} + \frac{1}{d}$. Since

$-\frac{1}{k-1} \left(\frac{2}{d}\right)^{k-1} < 0$ and $\frac{1}{d} < 1$, we get that if $d \geq \frac{2^{k-1}}{k-1} + 1$, then the diameter of the Cayley digraph is exactly k .

ii) $d \geq 3$ is odd:

From the inequality $2(k-1) \left(\frac{d-1}{2}\right)^{k-1} > 2d \frac{d^{k-1}-1}{d^2-1}$ we get $d > \left(\frac{d}{d-1}\right)^{k-1} \frac{2^{k-1}}{k-1} - \frac{1}{k-1} \left(\frac{2}{d-1}\right)^{k-1} + \frac{1}{d}$. Clearly $-\frac{1}{k-1} \left(\frac{2}{d-1}\right)^{k-1} < 0$, $\frac{1}{d} < 1$ and $\frac{d}{d-1} \leq \frac{3}{2}$, thus if $d \geq \frac{2^{k-1}}{k-1} + 1$, then the Cayley digraph is of diameter exactly k . \square

4. Conclusion

In this paper we construct the largest known Cayley digraphs of odd diameter and large degree using semidirect products $\Gamma_k = H^k \rtimes_{\varphi} D_k$. Simpler semidirect products $H^k \rtimes_{\varphi} Z_k$ have been used before. It would be interesting to consider $H^k \rtimes_{\varphi} P_k$ for various subgroups P_k of $Sym(k)$. The most difficult part in this research is often proving that the diameter of a Cayley digraph is exactly/at most k .

Note that the product $H^k \rtimes_{\varphi} Sym(k)$ cannot be used to construct Cayley digraphs $C(H^k \rtimes_{\varphi} Sym(k), X)$ of degree d and diameter k unless the generating set X is quite large (which would decrease the order of a Cayley digraph in terms of d and k). For example if $|X| = cn$ for some $c > 0$, then the order of $C(H^k \rtimes_{\varphi} Sym(k), X)$ is $k!n^k = k! \frac{d^k}{c^k}$. Since the order of a Cayley digraph of degree d and diameter k cannot exceed the Moore bound $1 + d + d^2 + \dots + d^k$, it follows that for $d \rightarrow \infty$ one must have $\frac{k!}{c^k} \leq 1$.

Let us also mention that all known construction of Cayley digraphs are very far from the theoretical upper bound, leaving space for future research.

Acknowledgements

We would like to express our gratitude to the referees for all the valuable and constructive comments. Research of the first author was supported by the VEGA Research Grant number 1/0811/14 and the work of the second author was supported by the National Research Foundation of South Africa, Grant numbers: 91499, 90793.

References

References

- [1] M. Aider, Réseaux d'interconnexion bipartis orientés, Rev. Maghrébine Math. 1(1) (1992), 79–92.
- [2] V. Faber, J.W. Moore and W.Y.C. Chen, Cycle prefix digraphs for symmetric interconnection networks, Networks 23 (1993), 641–649.

- [3] H. MacBeth, J. Šiagiová, J. Širáň, Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups, *Discrete Mathematics* 312 (2012), 94–99.
- [4] L. Schoenfeld, Sharper Bounds for the Chebyshev Functions $\Theta(x)$ and $\Psi(x)$. II, *Mathematics of Computation* 30 (1976), 337–360.
- [5] J. Šiagiová, Approaching the mixed Moore bound for diameter two by Cayley graphs, *Australasian Journal of Combinatorics* 61(1) (2015), 73–81.
- [6] T. Vetrík, Large Cayley digraphs of given degree and diameter, *Discrete Mathematics* 312 (2012), 472–475.
- [7] M. Ždímalová and L'. Staneková, Which Faber-Moore-Chen digraphs are Cayley digraphs?, *Discrete Mathematics* 310(17-18) (2010), 2238–2240.